Before the
FEDERAL COMMUNICATIONS COMMISSION
Washington, D.C. 20554

In the Matter of	)	
	)	
Protecting Against National Security Threats to the Communications Supply Chain Through FCC Programs	)	WC Docket No. 18-89

COMMENTS OF PUERTO RICO TELEPHONE COMPANY, INC.

Puerto Rico Telephone Company, Inc., dba Claro ("PRTC"), by its attorneys, submits these comments in response to the Federal Communications Commission's ("FCC" or "Commission") Notice of Proposed Rulemaking[1] ("NPRM") seeking comment on a proposed rule that would prohibit telecommunications providers from using support from the Universal Service Fund ("USF") to purchase or obtain any equipment or services produced or provided by any company posing a national security threat to the integrity of communications networks or the communications supply chain. The NPRM also asks whether the Commission should take action towards non-USF-funded equipment or services produced or provided by companies that might pose national security threats to the nation's communications networks.

PRTC shares the Commission's commitment to maintain the security of U.S. communications networks and supports efforts to ensure that USF funds are not used in a manner inconsistent with national security. However, as explained in these comments, the Commission should defer action on the proposed rule to allow the U.S. government an opportunity to develop and implement a comprehensive federal policy on information and communications technology

[1] *Protecting Against National Security Threats to the Communications Supply Chain Through FCC Programs*, WC Docket No. 18-89, FCC 18-42, Notice of Proposed Rulemaking (2018) ("*NPRM*").

("ICT") supply chain risk matters. Currently, the Administration and Congress have various efforts underway to ensure the integrity of the ICT supply chain, and it would be counterproductive in the interim for a single federal agency like the FCC to implement unilaterally a proposed remedy to address perceived national security risks – no matter how well intentioned.

If the Commission decides to adopt the proposed rule, it should decline to extend the rule to maintenance and upgrades of existing equipment or services that are critically important to network functionality and security, and it should categorically exempt service providers that are subject to national security agreements or letters of assurance with the U.S. government (hereinafter, "mitigation agreements"). Lastly, the Commission should not mandate the removal of existing network equipment or devices, but if it were to impose such an extraordinary requirement, it should allocate USF funds to assist service providers with the replacement costs.

I. THE COMMISSION SHOULD DEFER ACTION ON THE PROPOSED RULE TO ALLOW THE ADMINISTRATION AND CONGRESS TO DEVELOP A COMPREHENSIVE FEDERAL POLICY ON ICT SUPPLY CHAIN RISK.

ICT supply chain risks are growing in size and complexity. Cognizant of these risks and their associated challenges, various executive branch agencies and Congress are actively considering appropriate remedial measures.[2] These measures are delicate in nature as they have international, diplomatic, and economic implications. As a result, a critical need exists for a comprehensive and uniform federal policy to address ICT supply chain risks, and the Commission should defer adoption of the proposed rule until such a policy is in place.

In February 2018, the Department of Homeland Security ("DHS"), which leads the federal government's efforts to secure the nation's public and private critical infrastructure information

[2] *See* U.S. Telecom Ex Parte, WC Docket No. 18-89 (May 25, 2018) (noting that "communications supply chain risk discussions very closely related to the issues set forth in the NPRM are currently taking place at the Department of Homeland Security, the Department of Commerce, and in Congress.").

systems against cyber threats and a member of Team Telecom, launched a supply chain cybersecurity initiative to identify cyber defense gaps.[3] As part of the initiative, DHS will work with stakeholders to provide actionable information about supply chain risks and mitigations to users, buyers, manufacturers and sellers of technology products.[4] Additionally, in May 2018, DHS released a strategy outlining DHS's approach to identifying and managing national cybersecurity risk.[5] The strategy provides DHS with a framework to execute its cybersecurity responsibilities during the next five years by reducing vulnerabilities, countering malicious actors in cyberspace, and making the cyber ecosystem more secure and resilient. As part of the strategy, DHS will partner with key stakeholders "to incentivize security and enable cybersecurity outcomes such as minimizing vulnerabilities and addressing supply chain risks."[6]

In April 2018, the U.S. Department of Commerce ("DoC") denied the export privileges of Chinese telecom equipment firm ZTE Corporation for seven years after finding that ZTE violated the terms of its 2017 settlement agreement stemming from a multi-year conspiracy to violate U.S. export controls and sanctions laws.[7] The NPRM specifically mentions ZTE as one of two companies that had been previously identified by the House Permanent Select Committee on Intelligence as posing a security threat.[8] However, the ZTE ban and, indeed U.S. policy on Chinese

---

[3] Lauren C. Williams, *DHS Developing Supply Chain Security Initiative*, FCW, Feb. 14, 2018, available at https://fcw.com/articles/2018/02/14/dhs-supply-chain-security.aspx (last visited May 31, 2018).

[4] *Id*.

[5] Press Release, U.S. Department of Homeland Security, Department of Homeland Security Unveils Strategy to Guide Cybersecurity Efforts (May 15, 2018), available at https://www.dhs.gov/news/2018/05/15/department-homeland-security-unveils-strategy-guide-cybersecurity-efforts (last visited May 31, 2018).

[6] U.S. Department of Homeland Security, Cybersecurity Strategy (May 15, 2018), at p. 23, available at https://www.dhs.gov/sites/default/files/publications/DHS-Cybersecurity-Strategy_1.pdf (last visited May 31, 2018).

[7] David J. Lynch, *U.S. Companies Banned from Selling to China's ZTE Telecom Maker*, WASH. POST, Apr. 16, 2018, available at https://www.washingtonpost.com/news/business/wp/2018/04/16/u-s-companies-banned-from-selling-to-chinas-zte-telecom-maker/?utm_term=.286f5766ccda (last visited May 31, 2018).

[8] *NPRM* at ¶ 4 (citations omitted).

technology companies, is in a state of flux as evidenced by the President's directive that DoC take steps to assist ZTE.[9] These discussions are taking place as part of high-stakes trade negotiations between the U.S. and China with enormous potential economic impact for both countries.[10]

Congress, too, is addressing ICT supply chain risk matters. Significantly, Congress has introduced the bipartisan Foreign Investment Risk Review Modernization Act, which would expand the jurisdiction and operational mandate of the Committee on Foreign Investment in the United States ("CFIUS") to more effectively guard against the risk to the national security of the U.S. posed by certain types of foreign investment.[11] As a result of the CFIUS review process, mitigation agreements between parties to a transaction and the U.S. government often provide the government with the right to review and approve certain network equipment and network equipment vendors in exchange for clearance of transactions that involve foreign investment.[12] Another example includes the approval by the U.S. House of Representatives of the FY 2019 National Defense Authorization Act ("NDAA"), which would bar federal agencies from using technology produced by certain foreign equipment manufacturers.[13]

In mid-May, the House Subcommittee on Communications and Technology held a hearing to better understand threats to the competition and national security of the telecommunications

---

[9] Damian Paletta, Trump Says He'll Spare Chinese Telecom Firm ZTE from Collapse, Defying Lawmakers, Wash. Post, May 25, 2018.

[10] Damian Paletta, Trump links ZTE rescue to larger trade talks with China, contradicting top aides Wash. Post (May 16, 2018).

[11] Foreign Investment Risk Review Modernization Act of 2018, H.R. 4311, 115th Cong. (2017); Foreign Investment Risk Review Modernization Act of 2018, S. 2098, 115th Cong. (2017).

[12] *NPRM* at ¶ 8 (citations omitted).

[13] National Defense Authorization Act for 2019 (HR 5515); John Eggerton, Broadcasting Cable, "House Approves ZTE, Huawei Ban From U.S. Government Systems; Would be phased in over several years" (May 25, 2018), available at https://www.broadcastingcable.com/news/house-approves-zte-huwaei-ban-from-u-s-government-systems. The bill requires each applicable Federal agency to develop a plan to implement the prohibition throughout the agency's supply chain and submit such plans to the appropriate Congressional committees.

industry, including the prevalence of foreign equipment in U.S. telecommunications networks and the U.S. Government and industry's response to these threats.[14] The hearing's Memo states that the Subcommittee will examine the role of standards bodies that set the rules for equipment providers and suppliers, consider risk management-based approaches to network security threats, and explore longer-term threats to global competition, which will necessitate the evaluation of U.S. domestic manufacturing capacity, foreign investment policy and engagement in standards-setting bodies.[15] There are other Congressional efforts underway.[16]

Unlike other Executive Branch agencies, the Commission does not have the specific expertise, staff, resources or access to intelligence necessary to establish criteria for determining which companies pose a national security threat to the integrity of communications networks or the communications supply chain. The Commission recognizes that certain Executive Branch agencies do have specific expertise in these areas and, for this reason, refers certain application to them.[17] Unilateral efforts by the Commission to make determinations regarding which companies pose a national security risk could quickly come into conflict with those by other Executive Branch agencies and lead to unintended regulatory, economic or diplomatic consequences.

---

[14] *Telecommunications, Global Competitiveness, and National Security: Hearing Before the Subcomm. on Communications and Technology of the H. Comm. on Energy and Commerce*, 115th Cong. (May 16, 2018).

[15] Memo from Comm. Majority Staff to Members of the Subcomm. on Communications and Technology, re Hearing entitled "Telecommunications, Global Competitiveness, and National Security," May 14, 2018, at pp. 3-4, available at: https://docs.house.gov/meetings/IF/IF16/20180516/108301/HHRG-115-IF16-20180516-SD002-U2.pdf.

[16] *See e.g.*, Fair Trade with China Enforcement Act, S. 2826, 115th Cong. (2018); Defending U.S. Government Communications Act, H.R. 4747, 115th Cong. (2018); Defending U.S. Government Communications Act, S. 2391, 115th Cong. (2018).

[17] *NPRM* at ¶ 8. Team Telecom includes representatives from DHS, the Department of Justice (including the Federal Bureau of Investigations), the Department of Defense, the Department of State, DoC and the National Telecommunications and Information Administration, the United States Trade Representative, and the Office of Science and Technology Policy. *Process Reform for Executive Branch Review of Certain FCC Applications and Petitions Involving Foreign Ownership*, IB Docket No. 16-155, Notice of Proposed Rulemaking, 31 FCC Rcd 7456, ¶¶ 4-8 (2016)

Given the complexity and sensitivity of the issues being addressed by the Administration and Congress, and that the Commission's expertise and resources on these matters are limited, development of a whole of government strategy would be more prudent than piecemeal measures. Thus, the Commission should defer action on the proposed rule to allow for the coordination and development of a broader and more comprehensive strategy to address ICT supply chain risks.

II. IF THE COMMISSION ADOPTS THE PROPOSED RULE, IT SHOULD DECLINE TO EXTEND THE RULE TO MAINTENANCE AND UPGRADES OF EXISTING EQUIPMENT OR SERVICES.

According to the NPRM, the prohibition on the use of USF support for the purchase of equipment or services produced or provided by a company posing a national security threat to the integrity of communications networks or the communications supply chain "would not apply to equipment already in place."[18] However, the NPRM also states that the Commission expects the rule to extend to "upgrades of existing equipment or services" and seeks comment on this view.[19] The Commission should reconcile this tension by declining to extend the proposed rule to maintenance of and upgrades to existing equipment or services.

The NPRM does not specify what activities would be covered by "upgrades" of existing equipment or services. Many upgrades, including maintenance and repairs, are necessary to preserve equipment functionality, performance, and security. These activities may include the purchase of spare parts, replacement or repair of damaged or malfunctioning components, hardware and software configurations, and the deployment of software upgrades. These activities extend the life of FCC-compliant equipment[20] and maximize the return on the equipment

---

18 *NPRM* at ¶ 18; *see also NPRM* at ¶¶ 2, 13 (stating that the rule would apply "going forward").

19 *NPRM* at ¶¶ 15, 18.

20 A service provider cannot import or market any RF device that does not comply with the Commission's technical requirements and such device bears an FCC ID as evidence of compliance. Carriers have invested considerable resources ensuring compliance with these and other equipment-related FCC rules.

investment. Thus, if the Commission adopts the proposed rule, it should specify that it will preserve the availability of USF support for maintenance and upgrade activities related to existing equipment and devices.[21] For the same reasons, the Commission should grandfather existing service contracts, including multiyear contracts and contracts for future upgrades and/or services.

Failure to allow USF recipients to maintain and repair their equipment would raise regulatory takings concerns. The U.S. Supreme Court has held that regulatory actions that deny "all economically beneficial or productive use" or deny an owner "economically viable use" result in regulatory takings.[22] A regulatory taking involves destruction of a company's "reasonable investment-backed expectations."[23] If providers are unable to maintain and repair their equipment, it will quickly become obsolete, depriving them of all economic and beneficial use and extinguishing investment-backed expectations. While property may be regulated to a certain extent, "if regulation goes too far it will be recognized as a taking."[24]

III. IF THE COMMISSION ADOPTS THE PROPOSED RULE, IT SHOULD EXEMPT SERVICE PROVIDERS THAT ARE SUBJECT TO MITIGATION AGREEMENTS.

The NPRM appropriately seeks comment on whether certain categories or types of equipment or services should be exempted from the scope of the rule.[25] The Commission should exempt from the proposed rule any equipment utilized or services provided by USF recipients that

---

[21] The Commission should also limit the proposed rule to direct spending on prohibited equipment, devices, and/or services. If the rule were to extend to USF funding of entire projects that utilize specific equipment, devices, or services, service providers would be required to replace substantial portions of their networks and/or devices.

[22] *Lucas v. S.C. Coastal Council*, 505 U.S. 1003, 1015 (1992).

[23] *Penn Cent. Transp. Co. v. City of New York*, 438 U.S. 104, 105 (1978).

[24] *Pennsylvania Coal Co. v. Mahon*, 260 U.S. 393, 415 (1922).

[25] *NPRM* at ¶ 15.

are parties to mitigation agreements, by which their networks, equipment, and traffic management practices are subject to U.S. government oversight.

As previously noted, the Commission will seek the views of Team Telecom as to whether an application poses national security, law enforcement, foreign policy, or trade concerns because of its expertise in these areas. After the agencies review an application, they may file comments requesting that the Commission condition grant of the application on compliance with a mitigation agreement or deny the application.[26] While mitigation agreements are specific to each company, they are specifically designed to alleviate potential national security, law enforcement and/or public safety concerns. As such, common provisions include: (a) access by national security agencies to detailed network information including principal equipment and network management practices; (b) site visits by national security agencies; (c) filing annual reports with updated principal equipment lists and network architecture and control diagrams; (d) reporting network security breaches; and (e) prohibitions designed to ensure network security.

If national security agencies determine that a service provider's network, equipment and traffic management practices do not pose national security, law enforcement and/or public safety concerns, the Commission should defer to this determination, which would obviate any need to apply the proposed rule. As the NPRM states, the Commission seeks input from the Executive Branch agencies precisely because of their specific expertise regarding national security, and no purpose would be served in the Commission disregarding the exercise of their expertise.[27]

---

[26] *NPRM* at ¶ 8.

[27] A less desirable alternative to a categorical exclusion could be implementation of a separate waiver process specifically designed for service providers with mitigation agreements in place. Because of the existence of the mitigation agreements, a waiver process should be limited to providing to the Commission, subject to confidentiality, evidence of the existence of such agreement. Confidentiality concerns, however, make a waiver process highly troublesome.

IV. THE COMMISSION SHOULD NOT PURSUE OPTIONS THAT WOULD ENTAIL THE REMOVAL OF EXISTING EQUIPMENT.

The NPRM asks if the Commission should consider actions in addition or as an alternative to restricting the use of USF support, such as, for instance, "testing regimes, showings, or steps concerning the removal or prospective deployment of equipment."[28] For the reasons explained below, the Commission should not require the removal of existing equipment.

Mandating the removal of existing equipment purchased with or without USF funds would be troublesome for several reasons. First, by reaching equipment already installed, it would contradict the Commission's statement that application of the proposed rule would be prospective only. Second, it would raise questions regarding the Commission's legal authority to deprive companies of their property. Third, the expenses associated with such a mandate would be extraordinary and would include, at a minimum: (a) lost opportunity cost in decommissioning otherwise good equipment; (b) the physical removal of existing equipment and attending network; (c) the legal costs associated with termination of maintenance and repair service agreements; and (d) the purchase and installation of replacement equipment. Fourth, as with the proposal that would prohibit USF recipients from maintaining and repairing their equipment, mandating the removal of existing equipment would raise regulatory takings concerns. For these reasons, the Commission should not pursue national security steps that would entail the removal of equipment.

However, if the Commission were to direct the removal of existing equipment, it should allocate USF funds specifically designed to assist service providers with the expense of removing the existing equipment and purchasing new equipment.

---

[28] *NPRM* at ¶ 31.

V. CONCLUSION

PRTC agrees with the Commission's stated objective of ensuring that universal service funds are not used in a way that undermines national security. As it moves forward, however, the Commission should give due deference to relevant Administration and Congressional efforts addressing the integrity of the ICT supply chain, and decline to make unilateral determinations regarding which companies pose a national security risk. If the Commission decides to adopt the proposed rule, it should narrow its scope and reach as explained in these comments.

Respectfully submitted,

/s/ Francisco J. Silva
Francisco J. Silva
General Counsel
Puerto Rico Telephone Company, Inc.
1515 F.D. Roosevelt Avenue
Guaynabo, PR 00968

June 1, 2018